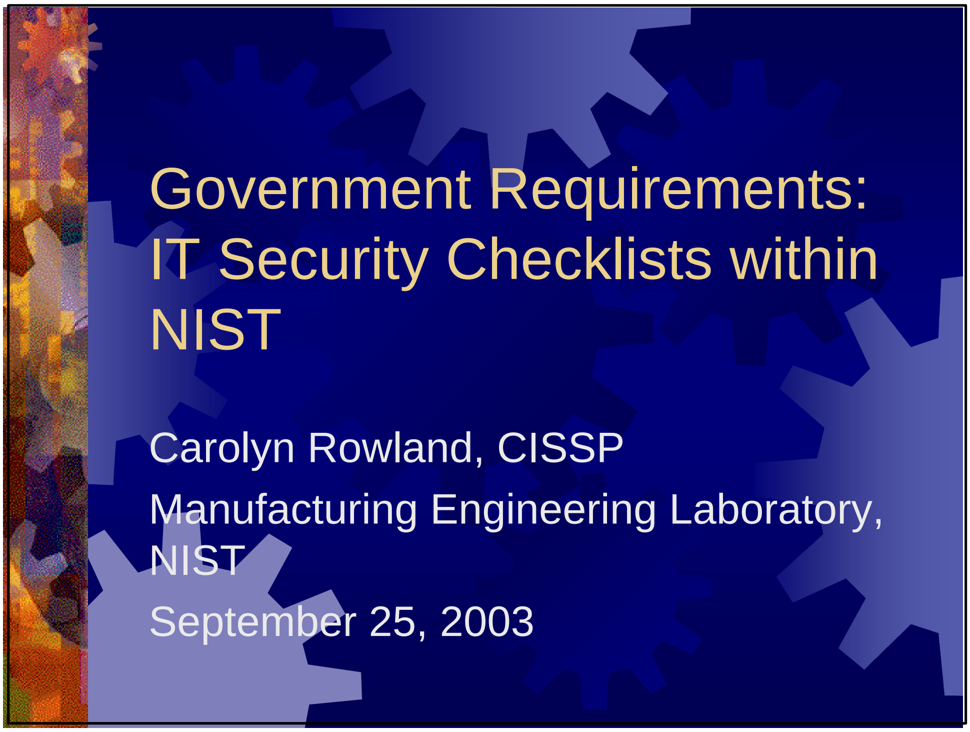
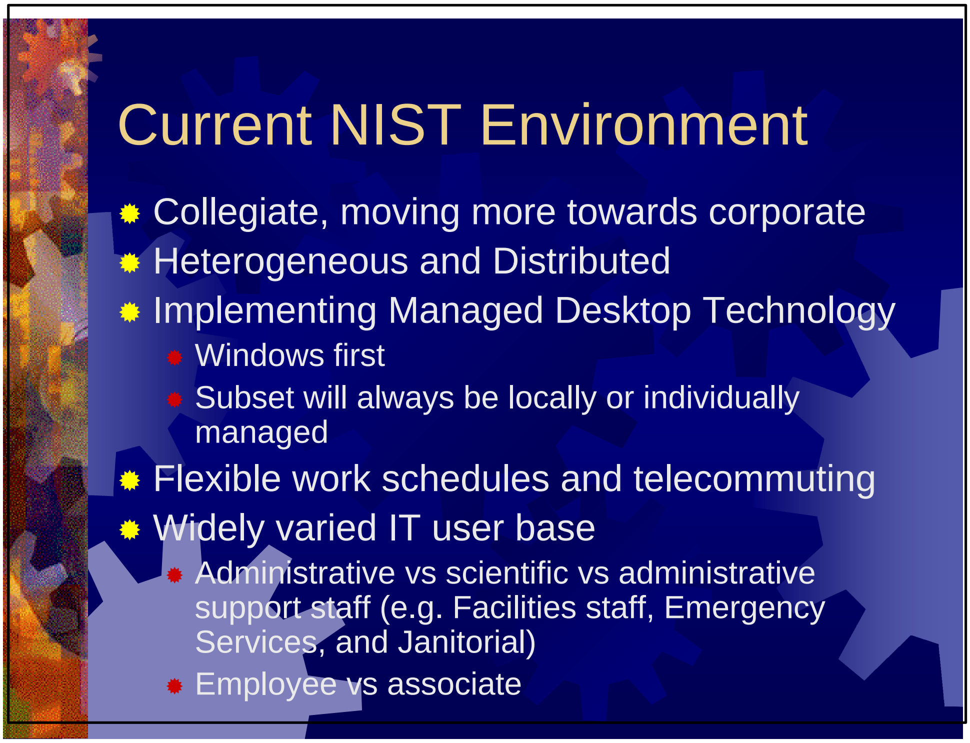


Government Requirements: IT Security Checklists within NIST

Carolyn Rowland, CISSP

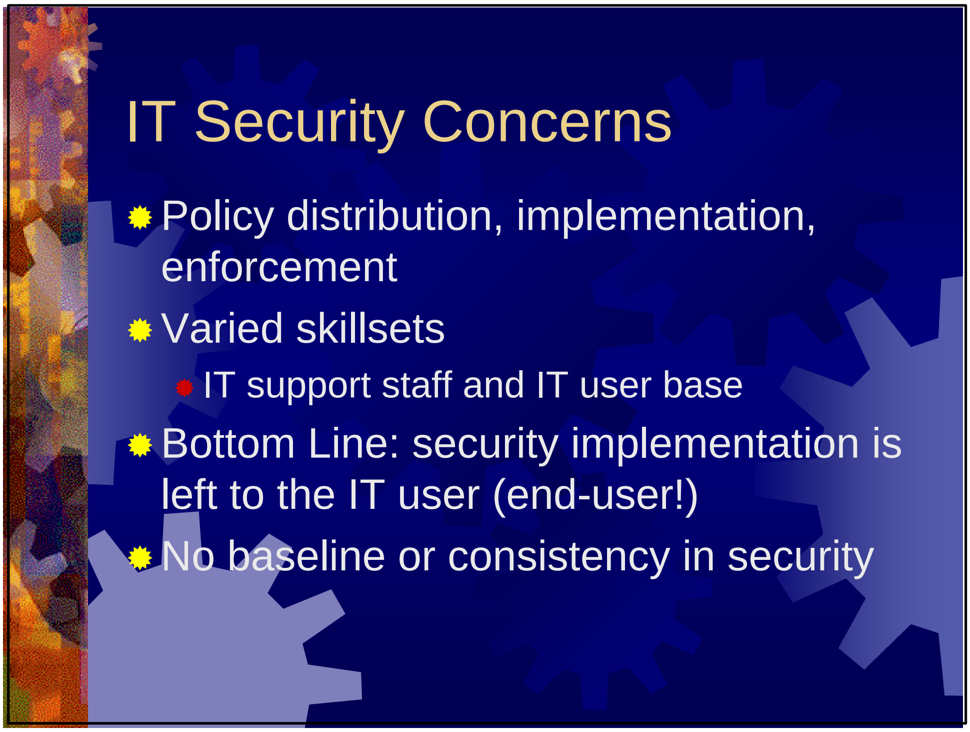
Manufacturing Engineering Laboratory, NIST

September 25, 2003



Current NIST Environment

- Collegiate, moving more towards corporate
- Heterogeneous and Distributed
- Implementing Managed Desktop Technology
  - Windows first
  - Subset will always be locally or individually managed
- Flexible work schedules and telecommuting
- Widely varied IT user base
  - Administrative vs scientific vs administrative support staff (e.g. Facilities staff, Emergency Services, and Janitorial)
  - Employee vs associate

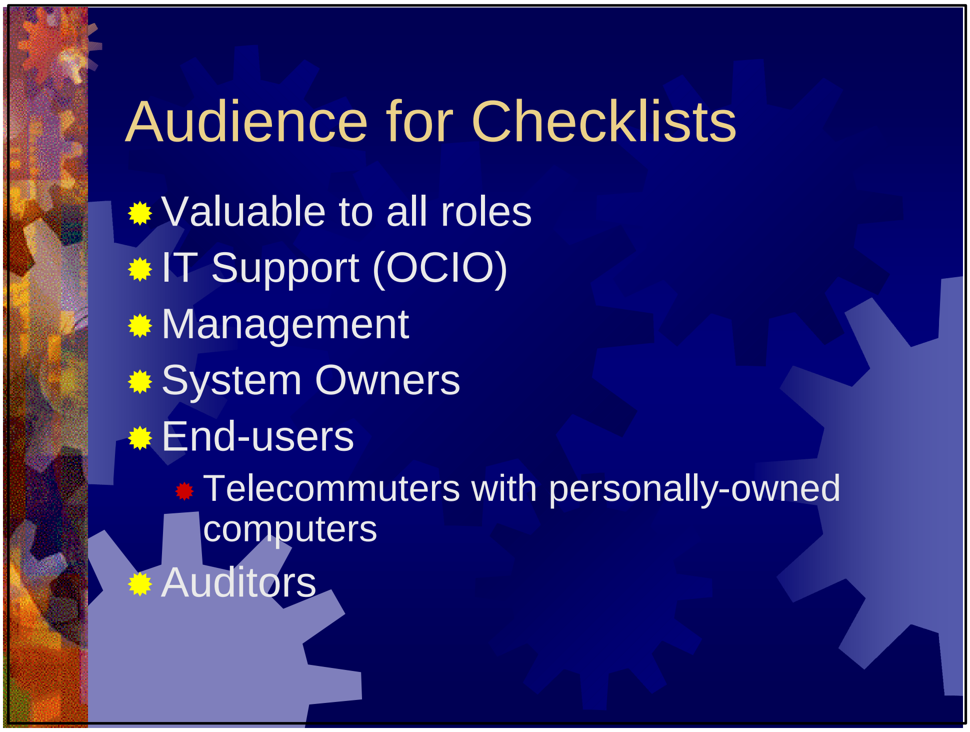


IT Security Concerns

- Policy distribution, implementation, enforcement
- Varied skillsets
  - IT support staff and IT user base
- Bottom Line: security implementation is left to the IT user (end-user!)
- No baseline or consistency in security

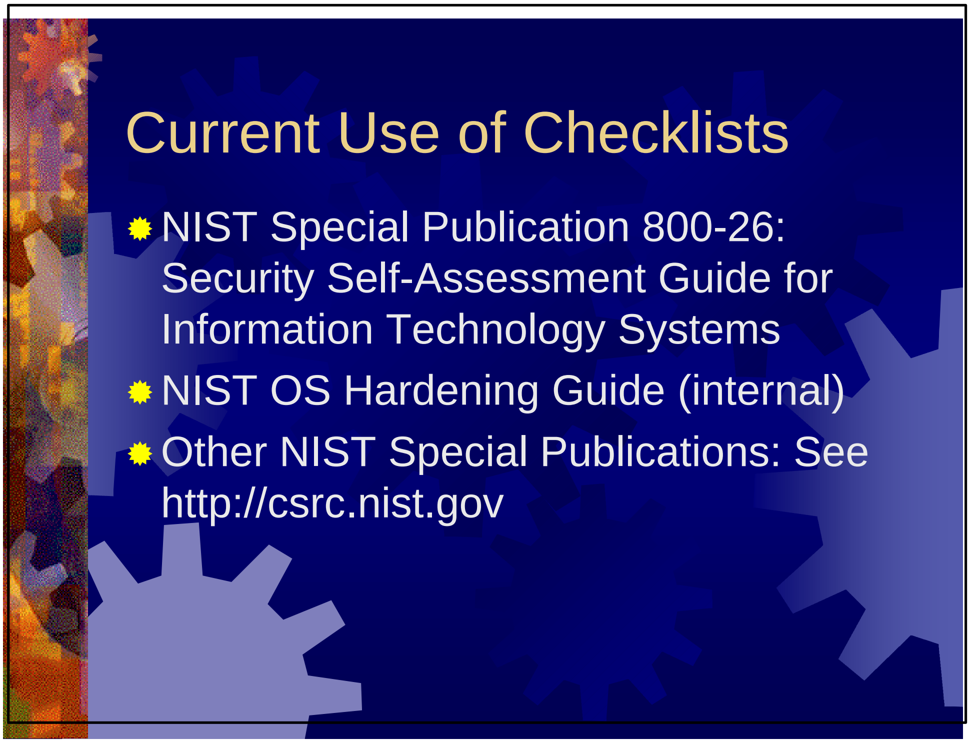
IT Security Checklists: Part of the Solution

- Empowers all roles
  - management, IT support, IT users
- Provides consistency of IT security: distributed installation causes various methods to be used
- Provides organization with documentation on level of security for IT resources (baseline)
- Improves organizational consistency through adoption of checklist and procedures
- Checklists make things easier



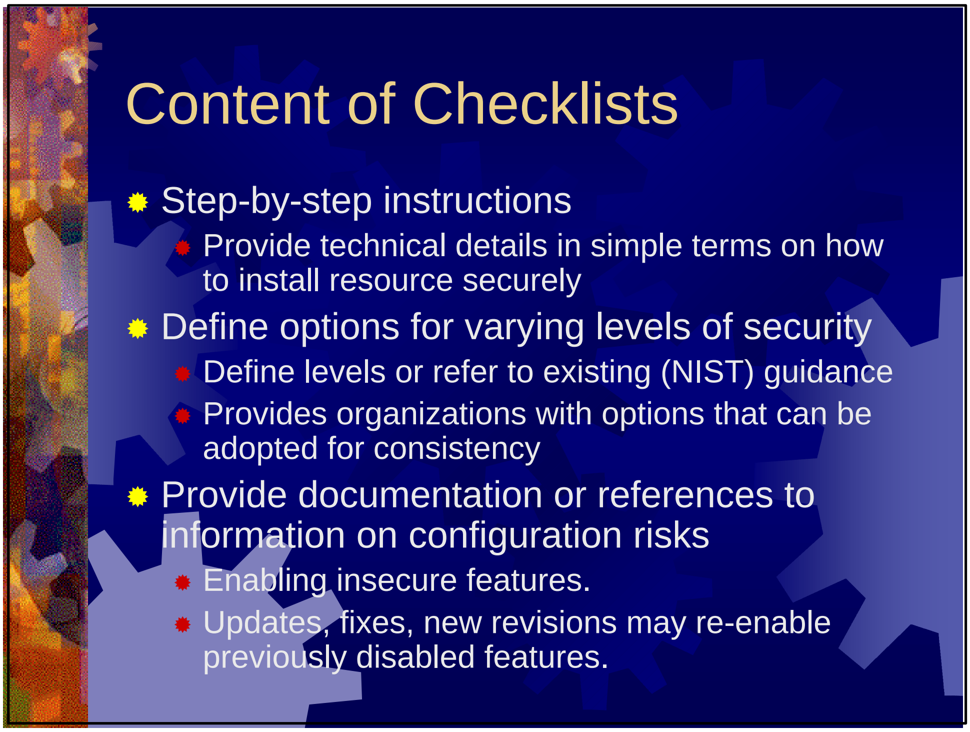
Audience for Checklists

- Valuable to all roles
- IT Support (OCIO)
- Management
- System Owners
- End-users
  - Telecommuters with personally-owned computers
- Auditors



Current Use of Checklists

- NIST Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems
- NIST OS Hardening Guide (internal)
- Other NIST Special Publications: See http://csrc.nist.gov



Content of Checklists

- Step-by-step instructions
  - Provide technical details in simple terms on how to install resource securely
- Define options for varying levels of security
  - Define levels or refer to existing (NIST) guidance
  - Provides organizations with options that can be adopted for consistency
- Provide documentation or references to information on configuration risks
  - Enabling insecure features.
  - Updates, fixes, new revisions may re-enable previously disabled features.